Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 57 (2015) 178 – 188

Procedia Computer Science

Impact of Signal-Strength on Trusted and Secure Clustering in Mobile Pervasive Environment

Madhu Sharma Gaur[a*], Dr. Bhaskar Pant[b]

[a]*Ph.D. Scholar GEU, Dehradun, Asst. Prof., G. L. Bajaj Inst. of Technology & Management. Greater Noida*
[b]*Asst. Prof, Deptt of IT, GEU Dehradun, pantbhaskar2@gmail.com*

Abstract

This Proposed work is further extension of our previous work, cluster based Soft Security trust metric evaluation in Mobile Pervasive Environment. Pervasive computing has the potential to provide low cost, high performance, and user centric solutions to exchange the information and communicate seamlessly in highly dynamic, heterogeneous environment where small and powerful dissimilar devices or nodes have to establish independent network unknown by the user. Communicating devices or nodes are resource-restricted and equipped with micro or bio sensors to acknowledge the signals. To provide promising level of security assurance traditional security systems based on cryptography and encryption are not sufficient. In this paper we present extension of our previous work where we observe node's impulsive behavior to become malicious as a soft security factors and propose a trusted cluster formation with security and energy efficiency considerations in the subjective area. In this work we analyses impact of signal-strength attacks while cluster communication on trust degree and level of security. In winding up, we put our efforts to validate the proposed approach and present comparison with other similar schemes for significant adaptation of trustworthy and secure communication where information is ubiquitous.

Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

Keywords— Clustering, Mobile Pervasive Environment, Security, Signal Strength, Trust

1. Introduction

In the decentralized and highly dynamic environment like Mobile Pervasive Environments (MPE) trust and security measurement are two major challenging issues where small, powerful and resource-restricted(limited speed, storage and power backup) devices are communicating seamlessly. In spite of these constraints and due to no fixed infrastructure a self-adaptive and self-organizing configuration is the required to adapt dynamic topology in such environments. Standard clustering technique is one of the most renowned

* Corresponding author.
E-mail address: madhu14nov@gmail.com

Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)
doi:10.1016/j.procs.2015.07.418

and encouraging energy-efficient technique for improving the scalability against heterogeneous scenarios, where grouping of nodes is formed as a cluster. In a clustered network, a node that coordinates the cluster activities is known as cluster-head (C-Hd) and other nodes inside the cluster, are called member nodes. The member nodes can directly communicate with the C-Hd. The C-Hd generates a TDMA (Time Division Multiple Access) sending message frame and sends it to its member nodes, and also use some gateway nodes which act as bridge between different clusters. There are mobile hosts which can link to the network on the air and can be deployed rapidly with the potential of user-centric seamless communication. Furthermore, the self-adaptive, self-organizing communication can survive better in critical situation like war, terrorism, healthcare, home or natural disaster scenarios compared to fixed infrastructures.

Our earlier work focus on trust based soft security with the assumption that strength of security assurance can be enhanced by identifying strong and weak trust parameters as trust metric used for a trusted cluster formation. In this paper, we explore security concerns and challenges to identify the impact of signal-strength or attenuation attacks as a further extension to provide trusted and secure cluster communication. Prevailing clustering algorithms based on the assumptions of an ideal network with no signal strength attenuation and generally fail to scale well in realistic highly dynamic environments. We assume that ever changing signal strength can be considered an important parameter for ensuring dynamic behaviour of a cluster. By exhibiting signal attenuation circumstances, the proposed approach parameterizes clustering criteria to estimate security assurance on trust credentials of a mobile node. A mobile node with maximum credentials has high probability to play as a cluster head to allow secure and trusted communication in resource-restricted and energy- efficient cluster. The major contributions of this work are -

- Exploring the trusted and secure cluster concerns and challenges to identify more security models in resource-restricted mobile pervasive environments.
- Ascertain the Impact of Signal Attenuation on Trust security evaluation
- Defining trusted and secure cluster communication with validation and comparison

The rest of the paper is organized as Section II describes the literature review. A note on Trusted and Secure clustering concerns and challenges is discussed in Section 3. S and in section III has been discussed. In the section IV we present the Proposed Approach where causes of signal attenuation and signal strength attacks due to attenuation has been recognized to evaluate the impact on trusted cluster and in the section V- we show Experiment setup, performance evaluation and comparison with similar existing models and finally in section VI Conclusion and future scope.

Figure1: View of Mobile pervasive environment

2. Literature Review

The security objective classically consists of requirements like confidentiality, integrity, availability (CIA) as per specifications and standards. Traditional methods concentrating solely on digital security are insufficient. In the literature [12-14,17,18], works used node ID, connectivity, residual battery energy, speed and direction of mobility, trust information of links, et al. as clustering criteria to select an appropriate node as the CH. However the situations of signal strength attenuation regions of geographical area haven't been considered yet, which is ubiquitous. SLEACH defined in [1] is the first secure version of LEACH protocol[1,4,7], which prevents sinkhole, selective forwarding and HELLO flooding attacks by using Security Protocol for Sensor Networks and MAC for authentication. It averts an intruder node that can be member or cluster head, but doesn't guarantee confidentiality and availability and opponent can attenuate network's throughput by disrupting the time slot schedule of a cluster. SS-LEACH, RLEACH [4,17] are the another variation of LEACH protocol to provide security when energy efficient is critical. It used stochastic multi paths cluster heads chains to communicate with the base station, to extend the network lifetime. In [4], authors highlight new research area for secure routing issue, in WSNs considering sensor nodes mobility and base station replication or mobility. Proposed work is inspired form LEACH protocol variation with mobility and cluster head node attacks due to signal attenuation concerns for more promising security assurance.

If a Sybil node exists then it has to perform the tasks of the identities it possess. So when it exceeds a threshold value then the Sybil node is detected. [14]. Existing algorithms are based on sharing encryption keys, RSSI based scheme presents a solution for Sybil attack based on received signal strength indicator (RSSI) readings of messages. Recent researches in Sybil defense mechanisms are based on Social network based schemes [6, 5, 21, 23]. These schemes use the trust structure embodied in the networks assuming that Sybil nodes can create arbitrarily number of identities and are poorly connected Trusted and Secure Clustering.

3. Security Concerns and Challenges

Pervasive environment is characterized by the low cost, high performance small and powerful dissimilar devices, communicate seamlessly in highly dynamic, heterogeneous. All the efforts in progress serve to eliminate the limitations and obviate inherent challenges of mobile equipment which cause security concerns. Trust is one of the important aspects of mobile and heterogeneous networks that enable the communicating entities to deal with uncertainty and increase the security assurance. There are plentiful definitions given to trust in literature reflected by reliability, utility, availability, reputation, risk, confidence and quality of service to co-operate a node which is requesting a certain service. In our previous work [18,19],we attempt to define a cluster formation based on trust metric soft security parameters for pervasive devices equipped with micro sensors called nodes to provide ubiquitous communication and information exchange. The network relies on base technologies and controlled by a Base Station (BS). The base station is a gateway of the Wireless Sensor Network (WSN) to the outside world and is assumed to have sufficient computational and communication capabilities. We assume the subjective Environment sensor nodes can be implanted on the human body or biometric security compliance sensors are used in devices, for monitoring and mapping dynamic behaviour of such devices with storage and energy constrained intangible to conventional computing.

3.1 Trusted and Secure Clustering

Sensor nodes are explicitly vulnerable to attacks as works in an open environment that could be anywhere in the world and the sensor data managers could be compromised. Our trusted and secure approach based on the reputations to dynamically detect and deny resources with simplified recommendations among trusted peers to local cooperative groups using standard clustering develop trust and assure security. Using context information and notions of neighbourhoods a node store relevant information. If any malicious or compromised behaviour is credited to any known entity, the fact can be reported back in the community where that entity is known to be a repeated group. Dynamic monitoring of the node's impulsive behaviour that leads malicious node detection based on fraudulent snooping of the communicating channels by two inherent properties, firstly each node maintains a neighbour list containing the addresses of those nodes with which it is in immediate proximity or on the path from a source to a destination.

For trust computation [18, 19] we consider that each node maintains a table to keep its social and QoS trust factors as per their dynamic behaviour between communicating node like X and Y for time t that is autonomously updated while interacting with other nodes on demand or expiry to save resources. The Trust calculation between of two nodes in respect to the trust factors and mean of trust value based on each parameter as per predefined threshold. We Intimacy, Integrity, mobility selfishness and reliability as our trust metric parameters and Thus trust value that node X evaluates towards node Y at time t, $T_{xy}(t)$, is represented as a real number in the range of [0, 1] where 0 indicates distrust and 1 complete trust. As per [19] equation (1) Trust $T_{xy}(t)$ is computed by:

$$T_{xy}(t) = C1*T_{xy}^{Intimacy} + C2* T_{xy}^{Intigrity} + C3* \quad T_{xy}^{Energy} + C4T_{xy}^{selfishness} + C5T_{xy}^{Reliability} \qquad (1)$$

Where C1, C2, C3, C4 and C5 are costs associated with these five trust factors with equal threshold of 0.2 for each factor and C1 + C2 + C3 + C4 + C5 = 1. Deciding the best values of C1, C2, C3, C4 and C5 to maximize system performance is a trust formation.

3.2 Security Concerns and Challenges

- Connection Swings with limited Bandwidth: High mobility causes the fast change in topology to base stations and access points affects the signal quality that may low down the signal strength can lead to security attacks and threats.
- Cluster head with strong signal strength: C-Hd with strong signal strength possibly reduces bandwidth usage and packet broadcast overhead, and ensures that the CH cannot be easily replaced after the topology changes because mobility characteristics are detected that may also lead to security attacks.
- Malicious node Behaviour: A selfish or compromised node may make a routing service as a target service in ad hoc environment with attacks like attack on routing protocol or on packet forwarding or even on delivery mechanism aimed at blocking the propagation of routing information to a node or alarming the packet delivery against a predefined path.
- Transmission Range: Sensor nodes have limited transmission range due high desire of conserve energy.
- Fault Forbearance: Sensor nodes are always susceptible to the failures due to several of motives like Loss of battery power limited storage. Thus, researchers should also merge fault forbearance into their concepts and algorithms for improving the effectiveness of sensor networks.

3.3 Need for further Extension

Pervasive ad hoc Sensor Network is widely acknowledged technology for the twenty-first century where the deployment of mobile sensor nodes is carried out in an ad hoc fashion without cautious sensing electronics assessment of environment conditions through the sensor and transforms them into an electrical signal. Telecommunications industry has recognized the wireless mobile communication networks much more pervasive. In such networks signal transmission is one of the major causes of loss of signal strength in particular the transmitter power. Standard clustering technique has been also recognized an energy efficient approach for saving battery or device lifetime in such domains where pervasive ad-hoc networks are grouped together. In our previous work we propose a trusted cluster formation by selecting most trusted and energy efficient node known as cluster head i.e. is responsible for any communication with base station, another clusters through gateways and other member nodes. So far all reputation peer group and propagation has been performed by the cluster head. Cluster heads receive data from the cluster nodes, determine the appropriate reputation ratings for each node and send reputation reports back to the nodes. But there is very less work on monitoring or preventing the cluster head from being compromised node and performing malicious activities. Here we identify the cluster misbehaviour and attacks due the signal strength attenuation. To allow dynamic monitoring for cluster head to ignore information sending to the base station and false reputation reports about the member nodes in its cluster.

The trust degree explained in [2, 3, 13] so far is the part of trusted cluster formation that is now is intended to mitigate the false reputation attacks. In further work in progress first of all we identify the of significant causes for signal attenuation as signal passage thrashing that may lead to signal strength attacks on cluster head. Being a malicious cluster head; node makes routing services a target for routing attacks that can be either on routing protocol or on packet forwarding/ delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet

delivery against a predefined path.

4. Proposed Approach

The C-Hd with strong signal strength possibly reduces bandwidth usage and packet broadcast overhead and also ensures that the C-Hd can behave like malicious nodes due to signal strength attacks. As C-Hd can't be are easily replaced after every topology changes due high mobility. In a cluster when any event occurs, each cluster member node sends its sensor signal strength measurement to the C-Hd that will be used to perform event detection and localization. If the C-Hd will be malicious due to signal attenuation attacks then considerable impact will be on trusted cluster by security breaching attacks. We assume that ever attenuating signals can be monitored for ensuring dynamic behaviour of a cluster head node. By exhibiting signal attenuation circumstances, our proposed approach parameterizes clustering criteria to estimate security assurance on trust credentials of a mobile node. A mobile node with maximum credentials has high probability to play as a cluster head to allow secure and trusted communication in resource-restricted and energy- efficient cluster.

4.1 Signal Passage Thrashing

Signal passage is a pathway where signals actually travels and thrashing can be defined as disordered signal passage due to dropping of power density of an electromagnetic signal as it proliferates through the travelling environment. The signal passage thrashing can be also considered an important factor for signal strength attenuation. Here we identify following signal thrashing causes that may lead to attenuate the signal strength

- Open Gap Thrashing: It occurs as the signal travels through holes even without any attenuating effects; the signal diminishes on general propagation as the radio communications signal dispersal in an ever increasing sphere. As per conservation of energy, with the larger area, the energy will reduce as the area covered becomes larger.
- Topography: The topography over which signals travel will have a noteworthy effect on the signal. Apparently hummock area obstructs the passage for significant signal attenuation or even makes reception impossible.
- Assimilation Thrashing: Such kind of signal thrashing occurs when signal passes into a channel which is not totally transparent to radio signals just like light signal passing through transparent glass.
- Dissipation Thrashing: When an object come into sight in the pathway. The signal can diffuse in the region of the object; meanwhile some signal strength losses and if there are more rounded object the losses are much higher. Sensor nodes radio signals have a propensity to diffract larger around sharp edges.
- Multiple Pathways: In real global surroundings, signals reflected and follow the different pathways that may attach or deduct from each other based on the relative phases of the signals. Especially with high mobility pervasive devices overall acknowledged signal may change with the current position.
- Other Environmental Obstructs: For sensor based mobile devices applications and services, along with geographical environment other objects like buildings can also effect the attenuation of signal strength not only by reflection even by absorbing them.

4.2 Signal Strength Attacks

There are lots of Received Signal Strength(RSS) based algorithms have been proposed by community researchers and getting the attention for localization and reuse of existing communication infrastructure and are applicable to many commodity radio technologies. Such algorithms are still sensitive to various non-cryptographic attacks and the physical extent practices itself can be dishonoured by opponents like an attacker can implement signal strength attacks by placing an absorbing or reflecting factual signal reports. We attempt to formulate the all-around signal strength attacks, where similar attacks are launched towards all landmarks, and experimentally show the feasibility of launching such attacks. We then propose a general principle for designing RSS-based algorithms so that they are robust to all-around signal strength attacks.

A sensor node is able to receive the stimuli only if the signal strength power of the received packet is above a certain threshold. The propagation model configured at the sensor channel determines the attenuation of the signal and the received signal strength use Seismic propagation model calculates the received signal power as a function of distance between sender and receiver and the attenuation factor. It

has been observed that with the fall in signal strengt various types of attacks that can violate security of ad hoc networks; in-depth discussion of all types of attacks is beyond the scope of this work. Some of the major identified attacks of sensor network are given below

- Sinkhole Attack: when an opponent's aims to attract the traffic from a particular area through a compromised node making it more striking to surrounding nodes with respect to the routing algorithms with large "scope of impact".
- Selective Forwarding Attack: These attacks are the consequence of sinkhole attack and more treacherous than sinkhole attack where a compromised node suppress the selective message forwarding.
- Sybil Attack**:** A malicious node which can exhibit multiple fake ID's to the network is called Sybil attack.
- Mote-class and laptop-class attacks: In mote-class attacks, assailant is a resources constraint node and laptop-class attacks, an opponent is much more powerful, disposes a large processing power with large transmission range and a sufficient energy reserve.
- Jamming: Such attacks inhibits with the broadcasting frequencies of the sensor nodes. If the opponent can block the entire network then that form inclusive DoS.
- Tampering: When an assailant may damage a sensor node by replace the entire node or part of its hardware to gain access to sensitive information is known as tempering.
- Spoofing: The assailant can cause difficulties for the network and create routing loops, catch the attention of or drive back the traffic, by creating false error messages.
- Wormholes: The opponent passageways communications received in one part of the network over a low latency link, to another part of the network where the communications are then replayed.

In the further discussion we mainly focus on sink hole, selective forwarding and Sybil attacks in the reference of trusted cluster head and member nodes for pervasive ad-hoc sensor networks.

4.3 System Model

The low-energy adaptive clustering hierarchy (LEACH) protocol uses the first order radio model based and randomized rotation of cluster heads to facilitate the even distribution of energy among all sensor nodes. Due to exponentially attenuation of signal strength, the influencing area of each target is limited. However, when two objectives come closer to each other and their impelling areas overlap, the sensor nodes may form a single cluster rather than two separate clusters. To reduce the re-clustering rate and improve the stability and reliability of the transmission path, we use signal strength as the key concern for security assurance in a trusted cluster. There are three stages in our proposed approach as in first one Trust calculation stage, in second security evaluation. First of all nodes dynamic behaviour is evaluated as per trust parameter establish the trusted link between them. After that each sensor node broadcasts it's ID and also receives from its peer nodes that need to be checked with base station to verify compromised nodes to Sybil attacks and such nodes will be dropped finally trusted secure cluster formation will be done.

To use the signal strength value received by nodes as a clustering criterion, we define signal strength threshold In order to deal with the misbehaviour of cluster head node due insider assailants for routing security in cluster, in this paper we propose Peer/Wall Alert (PWA) considering the three most dangerous attacks sink hole attacks, selective forwarding and Sybil attacks, especially when applied by C-Hds attackers, due to high impact on network performance. In contrast with the most existent IDSs or all energy-expensive alerting systems, where alert messages are directly sent to the base station on each intrusion detection, our IDS presents a lightweight alerting system, composed of two types of alerting messages: Peer and Wall alerts. Peer alerts have a less energy cost, can be generated on regular intervals while wall alerts are raised occasionally, depending on threshold accomplishment. Our PWA is anticipated to be incorporated into secure routing protocols to meet the different requirements in particular low energy and resource constrained devices. At the Base station a data structure named Alert Manager (AM) will be used to maintain the information about the all nodes primarily node ID with signal strength as per predefined threshold and alert methods PWA. Whenever any node comes into the range with connection request, first it will be verified as per threshold. The AM will be initialized by identifying the node. Each sensor node dynamically monitored and list of compromised nodes or blacklisted nodes is maintained for a cluster to avoid making them cluster head in future. Sinkhole, Selective forwarding and Sybil attacks are detected dynamically after those member nodes transmit their communications. C-Hd in each cluster also get monitored, by hearing switched messages, during a period of time. If the finds that there is no data message sent by its C-Hd, this last is hereafter considered as attacker. Subsequently, the C-Hd's ID is put into blacklist, and disseminates a

peer alert message, containing the associated ID to the adjacent nodes in the clusters and blacklist is updated by adding assailant ID. In the detection algorithm, if any member node trust-cost in the previous list is less than the predefined threshold, the peer node is detected suspicious and AM node broadcasts an inspection request message to other member nodes about the suspicious node as a sinkhole node. In the cluster the cluster head node maintains the list of its member nodes with the node ID and its location i.e. also maintained by with base station. Whenever cluster head C-Hd's communication to send and receive on member node request then the cluster head first compares this ID and location with base station list if any of the information conflicted the node is suspected with Sybil attack. Furthermore, it will take less energy for C-Hd to communicate with the neighbours if the received signal strength of neighbours is strong (the neighbours are closed to the CH if there is no signal attenuation). The Signal Strength of such nodes is also monitored. Generally source node sends a route request message to a destination node and a number of paths are available, then the node from its peer nodes. The source selects a path to the destination based on the route selection. In our approach for path selection source measures the signal strength of its peer nodes and assigns a C-cost of Signal Strength (CSS) to its peers. Lower the signal strength is the lower CSS. The source regularly maintains the CSS to imitate the signal strength of its peer. The signal strength between a node and its peer depends on factors such as distance, obstacles, and environmental conditions. When the signal strength is high, the percentage of packet loss is low and same in other way round. We define the different levels of CSS and assume associations between the signal strength and the proportion of packet dropped to find attacker nodes.

Weak CSS: The Lowest cost of Signal Strength, where attacks probability is highest.

Normal CSS: This an average cost obtained from all node 's cost-values of the communication links in the route from source to destination.

Strong CSS: Optimum cost obtained from all the Cost values of the communication links in the route from source to destination.

4.4 Detection of Attacks with Signal Strength Attenuation

In[7] authors proposed a system that uses the RSSI (Received Signal Strength Indicator) value with the help of extra monitor (EM) nodes to detect sinkhole attacks [7,26]. The first theory for the detection of sinkhole attack was proposed by Ngai [4] that included the base station in the process of attack detection. Base station sends the request to get node ID to all the nodes in the network and node response with their IDs. The ID consist of the node position, next hop position and the associated cost. The information received is then used to build a network flow graph for identifying the sinkhole. Selective forwarding attacks are caused when malicious nodes refuse to forward certain messages and simply drop them, to not propagated in future. The opponent selectively forwards packets and concerned in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic. Similarly we propose the Dynamic Assailant Detection (DAD) algorithm for dynamically monitoring and Attacker detection in the subjective environment and also evaluate the impact of signal strength attenuation on it.

Dynamic Assailant Detection (DAD) algorithm:

Signal_Threshold: Predefined Signal Strength Threshold.
BLK_List: List of compromised or malicious nodes.
T_a: Time Taken in Assailant detection beginning.
Δtime: Period of time for dynamic monitoring
TDMA: Size of TDMA frame
Msg: Mmessage.
C_Hd : cluster head ID.
Begin
*$T_{a=}$ (Δtime) * TDMA) + random delay.*
if ((time = T) and (node-ID != C-Hd)) then
Provoke().
if (isMONITOR = true) then
Attend ().
if(C-Hd not allow Msg is heard) then
Blk-List=Blk-List+ID.
Msg [data] = C-Hd.
Peer(Msg).

```
    if ( (length (Blk_List) mod Threshold) = 0) then
    msg [data] = Blk_List
    Wall(Msg)  ;//directly to BS.
endif.
endif.
endif
endif.
```

As per the algorithm any node who's IDs seems in BlackList, will be discarded from cluster head and never taken in the future clusters reconstructions. Thus sinkhole attacks prevented and cluster nodes finding them compromised; detached from being transmitting false reports to the base station and avoid Sybil attack by avoiding fake IDs. The threshold value is chosen quite carefully so that it can reduce the black list updates overheads and to revoke the susceptible incoming malicious messages. Since the detection mechanism of our IDS is related to the ability of a AM to seize C-Hs's data message, it is possible that a false positive detection occurs and the C-Hd reports, normally, the data message to base station. Here we assume the bidirectional radio links between two peer sensor nodes based on Signal Passage thrashing; we calculate the distance between the transmitter and receiver with the effective proliferation loss like multi-path propagation and shadow fading. The signal propagation like lognormal shadowing model[8] can be used as shown below,

$$S(d) = P_T - P_R\,(d0) - 10\eta log10(d/d0) + X_\sigma \qquad (2)$$

Where, S (d) is the Signal value recorded at distance d, P_T is the transmit power, $P_R(d0)$ is the path loss for a reference distance d0, η is the passage Thrashing exponent, and X_σ is a Gaussian random variable with zero mean and $\sigma 2$ variance. This exemplify that if sensor nodes monitor radio signals, then no one can hide its location. Such as node X receives signal from node Y, then the Signal Strength is

$$S_R = (P_T.K)/(d_S)\alpha \qquad (3)$$

Where P_T is transmitter power at node Y, S_R Signal received, K is constant, d_S Euclidean distance between node X node Y. α is distance-power gradient. Suppose node Z receives radio wave from node Y at the same time, then the ratio of node Z to Y

$$S_{Ry}/S_{Rz} = (\,(P_T.\,K)/(d_{Sy})\alpha)/\,((P_T.K)/(d_{Sz})\alpha) \qquad (4)$$

At the time of network configuration and setup we assume that an opponent will not attack for first Time periods T_F, known as Safe Time, to study about the normal behaviour of the network like routing information, position of all sensor nodes.

4.5 Experiment Setup

To evaluate our approach, we experiment and simulated attacks. All the experiments show that our design principle can be applied to a wide spectrum of algorithms to achieve comparable performance with much better robustness. We simulate a Pervasive Ad hoc network with 500m X 500 m field with different pervasive devices or nodes 10 to 100 with random distribution. The sensors have radio range of 40m. A Base Station is at the top of the network to allow communication from the all the sensor nodes. The Routing Protocol AODV Data Rate 80 per 0.005 sec Packet Size 64 bytes Simulation Time 20sec using OPNet and SensorSimulator to show the results with different number of nodes in the network. As the number of nodes in the network increases, SensorSimulator is able to handle the traffic and the events generated in a better fashion so as to complete the simulation in a reasonable time faster than OPNet. We observe that as number of nodes increase the signal strength attenuation also increase with more attacker cluster nodes. Figure 2.1 ,2.2 and 2.3 shows with same number of nodes with different signal strength cost, the no of attacker nodes can be increased.

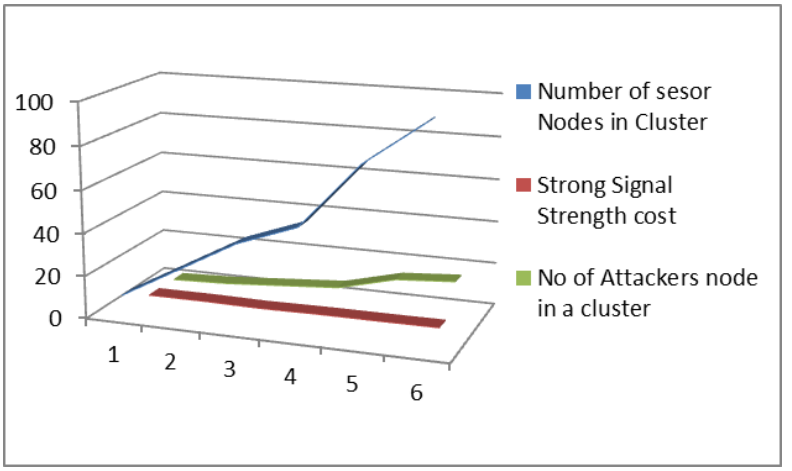

Figure2.1

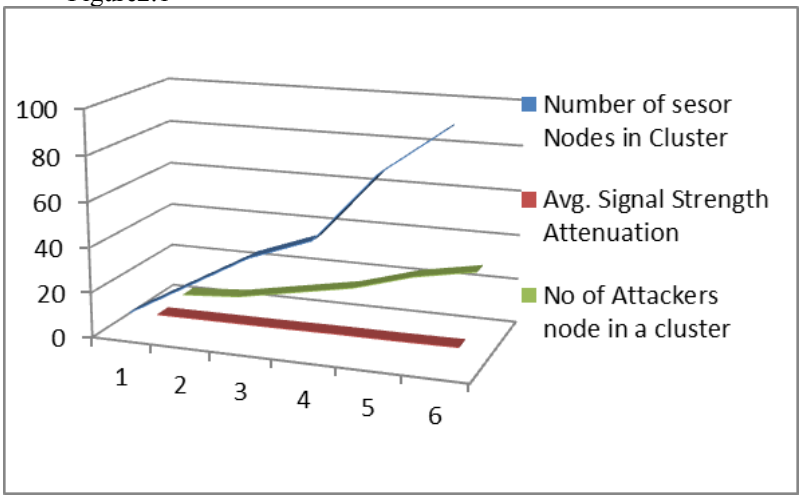

Figure2.2

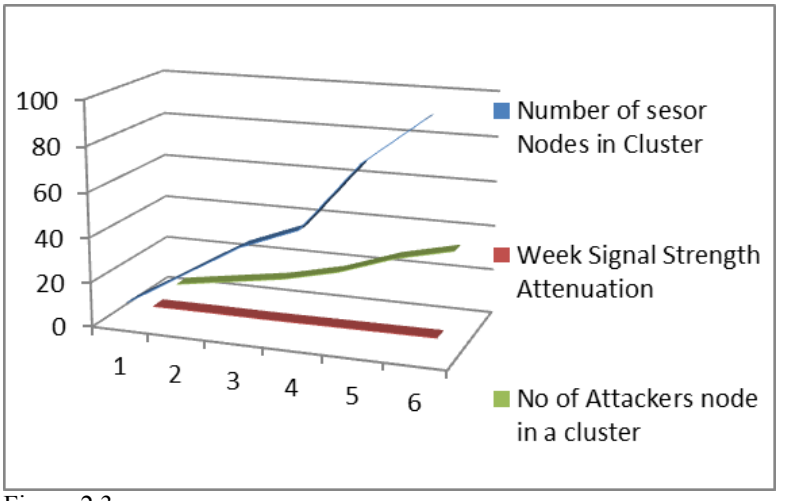

Figure 2.3

For comparison of results, between different variations of LEACH (ORLEACH, RLEACH and

LEACH) protocols, in term of the total delivered data to the base station, with the existence of variable and increasing number of compromised nodes attackers attempt to be CHs at each new cluster set-up phase, and exercise selective forwarding or black hole attacks is has been presented in figure 3 given below.

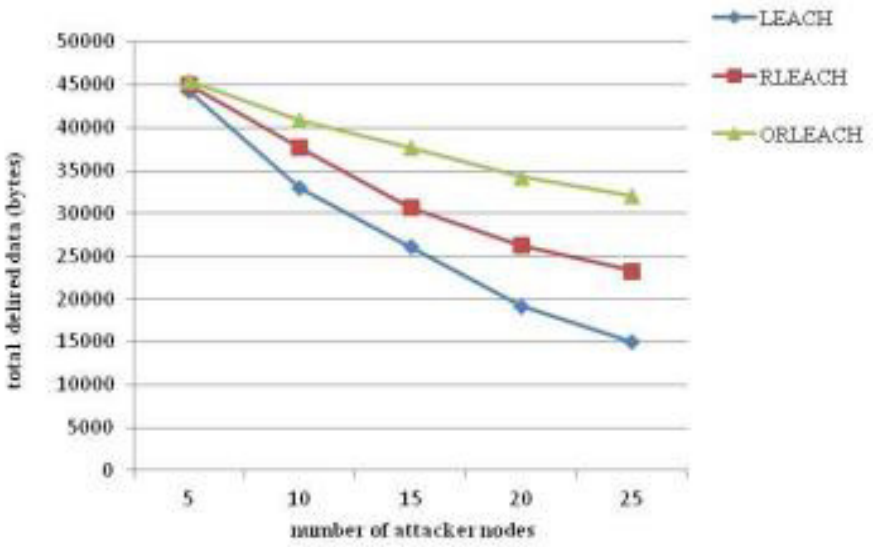

Figure 3: Comparison of number of packets delivered and attacker nodes [1,4,7]

5. Conclusion and Future Work

We have evaluated the signal attenuation attacks for a trusted cluster formation in mobile pervasive ad-hoc environment based on the dynamic behaviour monitoring of a node to become compromised and present the signal attenuation impact on cluster communication as a part of extended security consideration. To validate performance evaluation of the proposed approach and its comparison with the existing LEACH variation algorithms has been done. Designing a test bed using Sensor simulator or other network emulators implementation and acceptance in healthcare domain are steps forward to be taken to complete the journey all the way.

References

[1] A. C. Ferreira, et al, “On the security of cluster-based communication protocols for wireless sensor networks”,Fourth IEEE International Conference on Networking (ICNŠ), Berlin, pp. 449–458, 2005.

[2] Almenarez F., Marin A., Campo C., Garcia R.C. PTM: A Pervasive Trust Management Model for Dynamic Open Environments. Proceedings of the 1st Workshop on Pervasive Security, Privacy and Trust; Boston, MA, USA. August 2004.

[3] Almenarez F., Marin A., Diaz D., Sanchez J. Developing a Model for Trust Management in Pervasive Devices. Proceedings of 4th IEEE Annual International Conference on Pervasive Computing and Communications; Pisa, Italy. March 2006; pp. 267–271.

[4] A.M. El-Semary, M. M. Abdel-Azim, “New Trends in Secure Routing Protocols for Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, pp. 1-17, 2013

[5] BHARGHAVAN, V., DEMERS, A., SHENKER, S., AND ZHANG, L. Macaw: a media access protocol for wireless lan's. In Proceedings of the conference on Communications architectures, protocols and applications (1994), ACM Press, pp. 212.225.]

[6] Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel, Krishna P. Gummadi, Alan Mislove, and Ansley Post, “Exploring the design space of social network-based Sybil defenses”, IEEE 2012.

[7] C. Tumrongwittayapak and R. Varakulsiripunth, “Detecting sinkhole attack and selective forwarding attack in wireless sensor networks,” 2009 7th International Conference on Information, Communcations and Signal Processing (ICICS), (2009), pp. 1-5.

[8] D. Lymberopoulos, Q.Linsey, and A. Savvides, “An Empirical Characterization of Radio Signal Strength Variability in 3-D IEEE 802.15.4 Networks using Monopole Antennas”, In Proceedings of Third European Workshop on Wireless Sensor Networks, Springer Berlin, Heidelberg, Jan. 2006, pp.326-341

[9] D.Wu, G. Hu, and G. Ni, “Research and improve on secure routing protocols in wireless sensor networks”, Fourth IEEE International Conference on Circuits and Systems for Communications (ICCSC), pp. 853–856, Shanghai, May 2008.

[10] F. Li, P. Mittal, M. Caesar, N. Borisov, "Sybil Control: practical Sybil defense with computational puzzles", 7th ACM workshop on Scalable trusted computing, 2012.

[11] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho; Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, IEEE Transactions on Network And Service Management, Vol. 9, No. 2, June 2012

[12] Hamid Ali, Waseem Shahzad, Farrukh Aslam Khan, Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Applied Soft Computing 12 (2012) 1913-1928.

[13] Hsieh M.Y., Huang Y.M., Chao H.C. Adaptive Security Design with Malicious Node Detection in Cluster-Based Sensor Networks. Comput. Commun. 2007;30:2385–2400.

[14] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., Vol. 11, No. 1., Feb. 2004, 38-47.

[15] H. Yu, "Sybil defenses via social networks: a tutorial and survey, ACM SIGACT News, 2011.

[16] IEEE Communications Surveys & Tutorials, (2011), pp. 562-583.

[17] K. Zhang, C. Wang, C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management", IEEE Computer Society, pp. 1-5, 2008.

[18] Madhu S. Gaur, Bhaskar Pant, "Trust Metric based Soft Security in Mobile Pervasive Environment", in an International Journal of Computer Network and Information Security(IJCNIS), ISSN: 2074-9090:print (ISSN: 2074-9104 online,DOI: 10.5815/ijcnispublished by MECS Publisher, IJCNIS Vol. 6, No. 10, September 2014, PP.64-71,

[19] Madhu S. Gaur, Bhaskar Pant, "A bio-Inspired Trusted Clustering for Mobile pervasive Environment", Proceedings of the Third International Conference on Soft Computing for Problem Solving(SocPros 2013, Vol 2) of Advances in Intelligent Systems and Computing , organised by IIT Roorkee, Springer series AISC, ISSN-2194-5357. Volume 259, 2014, pp 553-564.

[20] Merin Achankunju, R. Pushpalakshmi "Quality Of Service Based Secure Clustering For Mobile Adhoc Networks Using Particle Swarm Optimization", in ITEE, Volume 2, Issue 3, June 2013, ISSN: - 2306-708X

[21] Nitish Balachandran, Sugata Sanyal,"A Review of Techniques to Mitigate Sybil Attacks", International Journal of Advanced Networking and Applications, 2012.

[22] Patwardhan, A., Parker, J., Joshi, A., Iorga, M., and Karygiannis, T. Secure Routing and Intrusion Detection in Ad Hoc Networks. In Proceedings of the 3rd International Conference on Pervasive Computing and Communications (Kauai Island, Hawaii, March 2005), IEEE, pp. 191.199.

[23] Wei Wei, Fengyuan Xu, "Sybil Defender: A Defense Mechanism for Sybil Attacks in Large Social Networks", Parallel and Distributed Systems, IEEE, 2013.

[24] Weiser, M. The Computer for the 21st Century Scientific American , September, 1991.

[25] WR Heinzelman, A Chandrakasan, H Balakrishnan, Energy-efficient communication protocol for wireless micro sensor networks. Proc 33rd Hawaii International Conference on System Sciences, 1–10 (2000)

[26] Wang Xin-sheng, Zhan Yong-zhao, XiongShu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009.

[27] TCG, "TCG MPWG Mobile Trusted Module Specification", version 1.0, Revision 7.02 29 April 2010.